

STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

**INFORMATION OPERATIONS:
TRAINING THE LEADERS**

BY

LIEUTENANT COLONEL MICHAEL FERRITER
Senior Service College Fellow, U.S. Army
Tufts University

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution is Unlimited

USAWC CLASS OF 1999



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

**INFORMATION OPERATIONS:
TRAINING THE LEADERS**

By

**Lieutenant Colonel Michael Ferriter
United States Army**

**Dr Richard Shultz
Project Adviser**

**DISTRIBUTION STATEMENT A:
Approved for public release. Distribution is unlimited.**

**U.S. Army War College
Carlisle Barracks, Pennsylvania 17013**

- The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

AUTHOR: Michael Ferriter (LTC), USA

TITLE: Information Operations: Leader Training

FORMAT: Strategy Research Project

DATE: 15 April 1999 Pages 17

CLASSIFICATION: Unclassified

The purpose of this project is to determine if the Army's officer education and training systems adequately prepare our leaders to operate within, and to deploy, fight, and win in the Information Age. As we depart the industrial age and enter the Information Age the United States Military is undergoing a Revolution of Military Affairs (RMA). I undertook this project to exploit the opportunity to study this area. In this project I describe and define Information Operations as they are defined by our doctrine. I place IO with the context of the strategic environment, and the role of IO across the Range of Military operations and spectrum of conflict. I review the Army's plan to establish and integrate information operations within the Army. I describe how the Officer Personnel Management System XXI (OPMS XXI) restructured the officer corps along related branches and functional areas. I assess the professional military education system's current and future plans to address IO and offer recommendations believe will assist the effort.

Introduction

What are Information Operations? I asked myself this question and several other questions. What should I know about Information Operations? Are Information Operations a battlefield function? Are they a condition under which we operate? What training systems and schools within our professional military education are designed to prepare our leaders to understand, execute or support Information Operations? As we depart the Industrial Age and enter the Information Age the United States Military is indeed undergoing a Revolution of Military Affairs (RMA). The purpose of this project is to determine if the Army's officer education and training system adequately prepares our leaders to operate within, and to deploy, fight, and win in the Information Age.

In this project I provide the doctrinal definition Information Operations.¹ I describe the strategic environment of the Post Cold War world in which asymmetrical threats, non-state and sub-state actors and ethnic and religious conflict have replaced the bipolar world dominated by two super powers. I address the effects of the RMA and information age technology within the Global Information and Military information environments.

Key to accomplishing this study is to define Information Operations (IO). From the beginning of the study I found there are so many things believed to be Information Operations and Information Warfare that I found it difficult to discern how this field is organized and managed.² It is impossible to determine what the education requirements would be until IO was defined. Once I define IO, I'll describe OPMS XXI and its impact on officer assignment, training and education. Finally I'll assess education and training I believe key to integrate Information Operations within our Army.

"Generally, in battle, use the normal force [direct approach] to engage; use the extraordinary [indirect approach] to win." Sun Tzu, *The Art of War*,³

The Strategic Setting: The RMA and the Explosion of Information Technology

As I began my journey on this study I found there are many definitions and many beliefs and even myths of what activities fall into Information Operations. Some believe IO are stand alone operations able to achieve stunning battlefield victories, while others believe IO are before, during and after conflict activities taken to set favorable conditions or shape the battlespace. These advocates see IO as an integrating process that synchronizes information with primary battlefield functions and makes success more easily achieved. I met with a variety of officers during my interviews and found that IO equates different things to different people. There are three categories: Computers, Sensors to Shooters and Digitization, Situational Awareness that dominate the informal tabletop discussions about Information operations. These are not the precise doctrinal components of IO, but are so often included in discussions I present them now, and will clarify later where each fits into the established components of Army Information Operations.⁴

Computers and Infosystems:

I met with several leaders whose units focused on computer network protection and attack and exploitation of our opponent's computers and information systems. Some of their activities fall into a classified realm of Special Information Operations.⁵ Other activities provided Infosystems that can speed decision-making by streamlining information management. The common belief is that soon commanders and their units will be able to operate during a conflict with a common picture of the battlefield provided through the technologies emerging in new infosystems and intelligence systems. These land, air and space based sensors will be able to record current friendly force positions and report with certainty locations of the enemy forces. This certainty will allow network linked fire control systems to instantaneously direct firing platforms to engage enemy forces. Some of this technology currently exists, but not in all units. The evolution and fielding of equipment and the associated manning, and development of tactics will continue and with it an increase in capabilities. At this time one can only predict that the authority to conduct computer futuristic network attack, and information infrastructure attack, will be withheld at the highest level of the military or even National Command Authority.

Sensors to Shooters and Digitization:

Many in the Army are strongly allied to the belief derived from a series of Army tests and experiments under the Army Warfighting Experiment (AWE). These experiments demonstrated how Information Age technologies and digitization provide total battlespace dominance and situational awareness. This segment of the military believes the information age and the RMA will provide us with a totally connected and continuously updated common picture of the battlefield. Ultimately, this new capability will change the way we fight. It will lead to highly lethal, much smaller organizations and allow for incredible dispersion on the battlefield. The theory is that if we know where we are, and where the enemy is; we can maneuver freely and can deliver highly lethal fires, with precision.⁶

Situational Awareness:

This synergistic effect of IO and information age technology is described in the Army's FM 100-6 Information Operations as follows: "In the past leveraging a knowledge advantage to decisively achieve a desired end state has largely been an intuitive process. Truly exceptional commanders have almost always possessed this trait. Information technologies now hold a potential for making this grasp of the battlespace and the inherent opportunities it affords more accessible to every leader. The effect of these changes will be to enhance battlefield visualization by better supporting leaders with deliberate and systematic information processes... Additionally, by linking commanders at different echelons, this same technology will enhance situational awareness and promote synchronized operational planning and execution. Ideally, the command will see and think as one"⁷

These systems include sensors and tracking systems that allow leaders at all levels to know exact locations of all friendly forces, when combined with intelligence systems and sensors that provide precise enemy locations the result is a certainty, an evaporation and reduction of Von Clausewitz's friction in war.⁸ Thus this certainty speeds decision making and provides combat leaders incredible speed in clearance of fires, and direct fire control and distribution.

Information Operations

“Information Operations are actions taken to affect adversary information and information systems, while defending one’s own information and information systems. IO require close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration and interaction of C2 with intelligence support. IO are conducted thorough the many capabilities and related activities. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include Computer Network Attack. IO related activities include, but are not limited to public affairs, and civil affairs activities.” Joint Pub 3-13

Army in Transition

We are currently in a transitional period. In the near term the most prevalent and likely Information Operations will be seen in MOOTW. These IO will be designed at the operational level to shape the battlespace in terms of public support locally, and to effect enemy and friendly morale.

Operations in Bosnia have demonstrated the results IO can achieve. Deploying staffs and headquarters have recognized the need for IO cells and have reorganized to accommodate this reality.

To assist in the transition, the Army’s elite Land Information Warfare Activity (LIWA) has served as a plug- in capability to deploying units to Bosnia. LIWA is the Army’s most experienced element in IO. The lessons learned in Bosnia are that an IO cell dedicated to integrate and synchronize the effects of C2W, OPSEC, deception, PSYOPS, Public Affairs, and Civil Affairs can be highly successful as a means to accomplish the commander’s intent in an operation.⁹ As a result, the Army has created IO cells in Major Commands (MACOMs), corps, and division headquarters level with authorized positions for permanently assigned IO personnel to serve as the commander’s IO staff. For the sake of this project, I’ll look at the training and education of three groups. The first are the integrators who provide IO support to the second group the line officers and commanders (the operators). The third group is the technicians, who design, install operate and maintain the infosystems¹⁰

Components of Information Operations

The Army identifies three interrelated components of I.O. They are Operations, Relevant Information and Intelligence (RII), and Information Systems (Infosystems). These components operate within a battlespace established by the Military Information Environment (MIE).¹¹

Information Operations = Operations + Relevant Information and Intelligence + Infosystems

All three components include six information activities:

1. Acquire Information
2. Use Information
3. Deny information
4. Exploit information
5. Manage information
6. Protect information

Operations

The first category of Information Operations is titled operations. These are military actions taken to use, gather, exploit, protect, or deny information in order to gain an advantage over an adversary. Information Operations define and shape the operational situation by generating understanding, providing context and influencing perceptions. Units conduct information operation across the full range of military operations, from operations in garrison, through deployment, to combat operations to redeployment. IO greatly expands a commander's battlespace, including interaction with the media, industry, joint forces, multi-national forces and computer networks worldwide. Command and Control Warfare (C2W), Civil Affairs (CA) and Public Affairs (PA) are the three operations the Army uses to gain and maintain information dominance and effective Command and Control.¹² ($\text{Operations}=\text{C2W}+\text{CA}+\text{PA}$)

Operations=C2W +CA+PA

C2W operations are the war fighting application of Information warfare. The aim of C2W is to influence, deny, degrade, or destroy information to the adversary. C2W directly supports the Army's goal of achieving information dominance and winning any conflict or succeeding in any MOOTW quickly, decisively, and with minimum casualties. C2W includes all or parts of the integrated use of operations

security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), and physical destruction. C2W is used to deny information to, influence, degrade or destroy adversary C2 capabilities while protecting friendly C2 capabilities.

The two disciplines of C2W are C2 attack and C2 protect. C2attack is the offensive C2W to gain control over our adversary's C2 function both in terms of flow of information and level of situation awareness. C2 attack is defined as the synchronized execution of action taken to accomplish established objectives that prevent effective C2 of adversarial forces by denying information to, by influencing, by degrading, or by destroying the adversary C2 systems.¹³ C2 protect seeks to maintain effective C2 of friendly forces by negating the adversary efforts to influence, degrade or destroy friendly C2 systems. C2 protect includes countering an adversary propaganda to prevent it from affecting friendly operations, public opinion and the morale of friendly troops. The commander and his staff must integrate five building blocks of C2W in order to achieve his (C2 attack and C2 protect) objectives. Again, these five elements are OPSEC, military deception, PSYOPS, EW, and physical destruction. Examples of C2 attack include activities that range from Cyber-combat and Computer Network attack targeted against an adversary's computer and information systems, banks and power grids, to conventional actions to physically destroy and damage command nodes.

The components of IO are not new. It is clear that this is a system of systems that needs to be integrated and synchronized. These systems are combat multipliers that must be employed in the new higher tech world. Some of these are new technology related and some are more traditional aspects of operations that can be more significantly exploited in the information age¹⁴

Operations=C2W +CA+PA

Civil Affairs

Civil Affairs activities establish, maintain influence or exploit relations among military forces, civilian authorities, and civilian populace in an Area of Operations to facilitate military operation. CA elements support military operations by applying their skills and experience in public administration, economics, public facilities, linguistics, cultural affairs and civil information and by collecting information relevant to the commander's critical information requirements (CCIR).

Civil Affairs activities encompass the relationship between military forces, civilian authorities and people in a foreign country in order to secure local acceptance of and support for US forces. CA is important to gain information because of its ability to interface with key organizations and individuals in the GIE; for example CA's traditional relationship with Non-Governmental Organizations (NGO's) and Private Volunteer Organizations (PVO's), such as the International Committee of the Red Cross. Commanders fully integrate civil-military operations (CMO) into all operations and use CMO to influence, coordinate, control or develop civilian activities and civil organizations.”¹⁵

Operations=C2W +CA+PA

Public Affairs:

The third component of operations is Public Affairs Operations. Today's modern press present combat operations nearly instantaneously. National and international news media coverage plays a major role in quickly forming public debate and shaping public opinion. The news media serves as a public forum for the analysis and critique of goals, objectives, and actions. The reality of near real time information has bridged the gap between what occurs on the ground and the goals and objectives of National Military Strategy. Public affairs officers monitor public perceptions and develop and disseminate clear and objective messages about military operations. PA works to establish the conditions that lead to confidence in and support of the Army. Commanders should plan for the presence of the media and provide effective interviews to communicate legitimate information to the public, strengthen soldier morale and unit cohesion, and enhance their ability to accomplish their mission. When integrated with other battlefield functions PA achieves the desired effect of an accurate, balanced, credible presentation of information that leads to confidence in the force and the operation.¹⁶

Operations are therefore military actions taken to create or achieve an informational position of advantage over an adversary or potential adversary. An example is by degrading an adversary's C2 nodes by C2 attack or physical attack an advantage is gained by way of IO. Another example is that the integration of friendly CA actions with preemptive PA messages can lead to friendly reception of our forces as they enter into a targeted area of operation. This is the form of Information Operations known for capitalizing on traditional functions within an integrated strategy. This integrated strategy is developed by the commander and his staff to use information to shape the battlespace. The command in these examples

maximizes the effects of information to assist in mission accomplishment through the coordination of C2W, deception, Psychological Operations (PSYOPS), Civil Affairs (CA), and public affairs (PA).

Information Operations = Operations + Relevant Information and Intelligence + Infosystems

Relevant Information and Intelligence (RII) provide the commander with the knowledge and certainty to act. As a category RII are the product (the information) of the Information Operations Category 1 (operations) provided, analyzed by, coordinated and communicated on the Information Operations Category 3 (Infosystems). RII is defined as information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the operational mission at hand.¹⁷

“Any military- like any company or corporation- has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information while selectively denying it to its adversaries and or allies.” Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century.

Information Operations = Operations + Relevant Information and Intelligence + Infosystems

Infosystems allow the commander to view and understand his battlespace, communicate his intent, lead his forces and disseminate pertinent information throughout his chain of command and his area of operations. Effective military and non-military Infosystems help the staff get the right information to the right location in time to allow the commanders to make quality decisions and take appropriate actions. Infosystems consist of the entire infrastructure, organization, personnel, and components that collect, process, store and transmit, display, disseminate and act on information

The role of Infosystems is to provide the infrastructure that allows the Army to interface with the GII. Infosystems enable the integration of all IO activities. Infosystems form the architecture that:

- Supports the staff process
- Supports the decision making process
- Provides the relevant common picture that helps synchronize force application
- Links sensors to shooters, and commanders
- Supports C2 attack and C2 protect capabilities.
- This area includes intelligence systems, sensors and systems that track friendly soldiers and units and give the commander battlespace dominance, and total situational awareness.¹⁸

Officer Professional Management System 21: OPMSXXI

Now armed with a keen understanding of the 3 components of Information operations, the question is who does IO involve? Who are the information operators? I'll define these as technicians, operators, and integrators. The Army's officer's corps are being reorganized under Officer Professional Management System 21 (OPMS XXI). OPMS XXI assigns these three groups into career fields and functional areas. My project focuses on the assignment and training of operators and the integrators. First I'll review OPMS XXI then the officer professional military education and training. This will reveal how the Army intends to train and educate its officers to perform in this Information Age and Information Operations. OPMS XXI assigns the officers into these four career fields:

- Operations Career Field (OPCF)
- Information Operations Career Field (IOCF)
- Institutional Support Career Field (ISCF)
- Operational Support Career Field (OSCF)

OPMS XXI restructures the Army competitive category by grouping interrelated branches and functional areas into officer management categories called "Career Fields". Officers will become expert in their field by way of repetitive assignments and career field related education opportunities. They will compete for promotion only with officers in the same Career Field. Below I provide a brief description of IO and Operations Career fields as they relate to the Army's Information Operations.¹⁹

Operations Career Field (OPCF) provides the Army with officers qualified by training, education and experience in areas directly related to the deployment and employment of land forces. It is composed of officers in the Army's 16 branches and 2 functional areas FA39 (PSYOPS/CA), and FA90 (Multifunctional Logistian Program). Officers who are designated in OPCF will command, while officers who are career field designated in other the other than OPCF are not eligible for command consideration.

Information Operations Career Field (IOCF) responds to the requirements of the 21st Century Information Age, consistent with Army Vision 2010, which identifies “Gaining Information Dominance” as fundamental to all future Army patterns of operation. The IOCF brings together related disciplines with associated functional areas and incorporates several new ones. The functional areas in the Career field are: FA24 (Information Systems Engineering), FA30 (Information Operations), FA34 Strategic Intelligence, FA40 (Space Operations), FA46 (Public Affairs), FA53 (Information System Management), and FA57 (Simulations Operations).²⁰

Each career field will have its own unique characteristic and development track for the officers who will respond to the readiness requirements of the Army today and into the 21st Century.

“While information operations always have been part of conflict, now in the high speed information Age, it has been significantly more important for commanders and command staffs to have dedicated personnel focus on information operations,” said LTC Ron Garner. He added “Officers assigned to FA 30 will be integrators, working across the entire spectrum of what a command needs in terms of offensive and defensive information operations, and drawing on the expertise of officers from other staffs.”²¹

Once assigned as FA30 IO specialists Captains will serve as IO targeting officers in divisions, combat developments staff officers, joint command watch officers, or as field support team officers with the Land Information Warfare Activity (LIWA). Typical jobs at the major’s level include Corps or division IO staff officers, LIWA field support team chief or IO officer Joint command headquarters or major Army command. FA 30 positions for Lieutenant Colonels will include IO coordinator at division level, IO plans officer for corps, division chief for LIWA and doctrine developer for TRADOC. Colonels will serve as IO coordinator for corps and Director of LIWA, IO division chief on the Army Staff and with joint and component, and major Army commands. The Army expects about a total of 180 FA 30 authorizations.²²

Much of the effort of IOCF will relate to information assurance, Computer network design and engineering, and computer network attack and protect. The Officers I described as the technicians,) will be assigned, trained and educated in these technical fields: FA24 (Information Systems Engineering), FA34 Strategic Intelligence, FA40 (Space Operations), FA53 (Information System Management), and FA57 (Simulations Operations).

Education and Training

The education and training process is evolving rapidly. The Army's Information Operations effort is led from the Army's Training and Doctrine Command. LTG Steele, Commanding General, Combined Arms Center (CAC), heads the Army's effort. He commands Fort Leavenworth and has organized an Information Operation Integration Contact Team (IOICT) that is made of nine working groups from members throughout the TRADOC community, the Army's Information Operations field and the Army at large. This IOICT is key and essential in sustaining the Army's progress in the many IO related areas and projects. Fort Monroe has partnership in the effort with its Information Superiority Division. Fort Leavenworth has an integration IO office at the CAC and Command and General Staff Officer Course. LIWA has provided a team of IO experts to LTG Steele to assist in the development of programs and instruction. These 9 working groups that meet or communicate monthly.²³

Working group # 1 is the Leader and Training Development. This working group is responsible to properly integrate IO into leader training. Below I will highlight the current programs, existing initiatives to increase or improve training, and then my recommendations. This is the training the FA30 personnel and the Army's operators are currently receiving and will receive. I chose a methodology of reviewing each level of training Officer Advanced Courses, Command and General Staff College, and War College because this allows one to follow Information Operations training integration along the normal levels of military education and officer career development.

Officer Advanced Courses:

Current status: Each branch school teaches what the specific branch contributes to IO. Example Signal School teaches the contribution of signal systems to communications, C2, C2W, Infosystems and computer networks. But they are not teaching how IO operations, as an integrated strategy, contribute to a commander's' mission success.

The plan for IO integration into the OAC is to insert into the OAC an IO common core training and training support package. The project is currently being developed and will begin in course instruction by 1st Quarter, FY2000. Linked to the Advanced Course is the Combined Arms Staff Service School (CAS3). As CAS3 primarily focuses on the Military Decision-Making Process and staff procedures it

offers a natural opportunity to build on the core training taught at the Advanced Course. CAS3 contains a 10-hour seminar. The seminar begins with an IO read ahead packet, and then presents to the CAS3 members of the Staff a scenario requiring an integration of an IO strategy into an operation.

Recommendation:

The core curriculum offered at the OAC will be the base education in Information Operations. I believe the Advanced Course should remain primarily focused on combined arms tactics, operations and leadership. The OAC does need to include the foundation core training in Information Operations. These officers will serve as principal battalion staff officers, and assistant staff officers at the brigade level, and action and watch officers at the division and higher level. They will be the first line of synchronization and integration of the battlefield functions and Information Operations. In the future they will be the commanders and operators who issue guidance and execute the plans. Providing a comprehensive core module provides the Army with a standardized core of future leaders who understand IO and its implications to all operations in the future.

The training should consist of definition of Information Operations, distinguish between Operations, Relative Information and Intelligence, and Information Systems. (Information Management, and Information Superiority). Special emphasis should be given within each of these three categories to the six information activities and their relations to the Military Decision-Making Process and existing staff procedures. The instruction should teach an understanding of how the OPMS XXI assigns officers to career fields and how these career fields interact with the three IO areas, Operations, RII, and Infosystems, and the alignment of the six functional areas, within the IOCF

Command and General Staff Officer College:

CGSC currently provides IO training imbedded into several courses. In the Division Operations Core Module there are several IO Enabling Learning Objectives. The Joint and Multinational Operations Module also incorporates IO training objectives. The Advanced Application Programs offer a classified Information Operations elective Course. This course is the highest quality IO instruction at CGSC because it highlights a cast of guest speakers active in the IO field and experienced in real world operations where IO played a significant role.

Recommendation:

CGSC is the first education level where officers designated in OPCF and IOCF join together to develop complex plans at the brigade, division and corps level. I recommend continuing the existing training and including IO into the end of year warfighter simulation.

The Army War College:

I attended the two-day seminar presented at the Army War College. It consisted of a read ahead packet of selected articles, guest lecturers, equipment displays, and seminar discussion. The guest lecturers were Directors from the Joint Command and Control Warfare Center and from the Land Information Warfare Activity.

Recommendation:

The War College should focus at the brigade commander and senior staff level. As this is an evolving field it is understandable the instruction I observed was general and familiarizing in nature. A core module of IO should be included to focus on commander's guidance and desired results. The instruction should include ongoing development of IO cells, IO targeting procedures and the integration of IO objectives into existing synchronization sessions. Guest speakers should be the general officers and former brigade commander who can speak first hand of IO lessons learned from recent operations.

Real World Application

Shaping the Environment

An example strategic shaping was vividly seen in the beginning of Operation Allied Force- the conflict in Kosovo. "NATO is not waging war against the Serbian people. We have no quarrel with the people—" Xavier Solana Secretary General NATO 24 Mar 99.

I sat and observed the NCA present the Ramboullait Peace plan through the national television media. Concurrently, the picture of suffering in Kosovo was painted clearly, leading to an undeniable understanding of the pain and suffering of Kosovo Albanians. The strategic environment was shaped artfully. The administration believed they would have to answer four concerns of the American people in order to gain support for Operation Allied Force:

1. Are vital interests at stake?
2. What are the chances of American casualties?
3. Why does America have to take the lead on this? Why isn't this a European problem solved by the European members of NATO?
4. What is the End State or End Game?

The press releases of 21-24 March 1999 were coordinated from the White House, Pentagon, NATO headquarters, and even from Richard Holbrooke in Belgrade. These reports before and at the outset of the conflict shaped the environment achieved congressional and public support for the NATO action against Slobodan Milosovic's regime and made us feel compelled to stop the pain and suffering even though some American casualties could be expected. This gives a real time example of how preemptive use of information power addressed the concerns and silenced the critics. As time goes on the air campaign employs C2W, and physical destruction of the Serbian C2 systems and television degrading the Serbian leader's capability to lead, and to inform his military and his people.

Army Leaders

The future paints a picture of an environment that requires military commanders who must be capable of operations along a spectrum of conflict. This conflict could range from one extreme of bloody close-combat conducted in internal wars within urban centers or out in rural areas. In contrast to that the

commander may just as easily find himself involved in Peacekeeping operations, where "condition-setting" information campaigns assist in maintaining the delicate peace. A third scenario could find the same leader embroiled in full-scale military operations characterized by the presence of the world wide press coverage, high tech weaponry, sensors and smart munitions. In light of these current conditions and the emerging technology and capabilities the combat leader will need to retain the core competencies of a warrior's leadership, and tactical expertise necessary to fight and win the bloody fights. This same leader will also need the competencies required to understand the information capabilities at his fingertips and how to integrate and synchronize these into his plans and operations.

Conclusion

Clausewitz highlighted the importance and yet the ambiguity of information when he said: "By the word information we denote all the knowledge which we have of the enemy and his country; therefore, in fact," the foundation of all our ideas and actions." He added: "Great part of information obtained in War is contradictory, a still greater part is false, and by far the greatest part is of doubtful character. What is required of an officer is a certain power of discrimination, which only knowledge of men and things and good judgement can give."²⁴

Imagine his surprise to see the accelerated growth of information, information sources, and information technology capabilities. Simply stated today's technology can provide the commander with increasingly precise friendly information and enemy intelligence. The commander and his staff will use the information to maintain situational awareness, and to issue timely and accurate plans and instructions to his units. This enhanced situational awareness provides a common picture of the battlefield and increased certainty which speeds the commander's decision cycle and will enhance his ability to defeat the enemy commander. This certainty allows the commander to know more, know first, and act first and decisively. Harnessing the potential of the Information to transform how the Army operates is critical to its success in the future. However, technology alone cannot provide leaders with automatic battlefield visualization, flawless situational awareness, easily expanded vision or highly effective information management. In the final analysis, the products of our initiative to harness the potential of information can only support the application of a leader's judgement wisdom, experience and intuition.²⁵

The Army remains responsible to fight and win the nation's wars. The Revolution in Military affairs is providing infinitely more precise firepower, fire control and situational awareness capabilities. The education and training systems will be required to keep pace with the technological innovations and introductions. The world will remain a volatile, and uncertain one with crisis and conflict spanning the full range of military operations and the full spectrum of conflict from peace to war. Our adversaries will also span a broad range from those who possess exceptionally high technologically advanced weaponry and systems to adversaries still fighting tribal and ethnic and religious wars. No matter who we face, it is clear to me there will remain a requirement for warriors who can fight and win close combat and stand on the high ground and hold it.

Endnotes

¹ Information operations is an evolving military field. I used FM100-6 which is under revision. The three components of Information Operations are defined in FM100-6 dated August 1996, as Operations, Relevant Information and Intelligence, and Infosystems. This project will use that categorization. The new FM100-6 is due for release and will categorize IO into two areas, Information Superiority and Information Management. I chose to use the categories in the current manual.

² As I began the interview process I discovered the vastness of IO. Some people live in a world of computer protection; others are dirty boots soldiers involved in shaping the commander's battlespace through the use of information in an integrated strategy designed to assist in accomplishing the commander's mission.

³ United States. Dept. of Defense, Joint Pub 3-13 Joint Doctrine for Information Operations. (GPO: Oct 1998) I-1.

⁴ Personal interview with Col. Brian Fredericks, ODCSOPS, Director, IO Division, 17 Dec 1998. Personal interview with John Giffin and Jim Winters, TRADOC IO Division, 8 Feb 1999.

⁵ USAWC Information Operations Seminars and guest speakers, 5 Jan 1999.

⁶ Hartzog, William W. Force XXI: Land Combat in the 21st Century (Virginia: U.S Army Training and Doctrine Command) Presented at the TRADOC capabilities display at the AUSA Annual Conference. Washington, 18 October 1998.

⁷ United States. Dept. of the Army, Field Manual 100-6 Information Operations (Washington: GPO 1997) 1-10

⁸ Carl von Clausewitz, On War, ed. Anatol Rapoport, (London: Penguin, 1988) 162-163.

⁹ Fredericks, B. Personal interview. 17 Dec 1998.

¹⁰ Telephonic interview 23 April 1999 with LTC Ron Garner, Chief of Functional Area 30 (Information Operations) Personnel Proponency Office, Combined Arms Center, Fort Leavenworth, Kansas.

¹¹ FM 100-6, 2-3.

¹² FM100-6, 2-3, 2-4.

¹³ FM100-6, 2-4, 3-2, 3-6.

¹⁴ FM 100-6, 2-4.

¹⁵ FM100-6, 2-5.

¹⁶ United States Dept of the Army FM46-1 Public Affairs Operations (Washington: GPO 1997) 13. FM100-6, 1-13.

¹⁷ FM100-6, 4-0.

¹⁸ Joint Pub 3-13, 6-0. FM100-6, 5-1.

¹⁹ The Army's officer's corps are being reorganized under Officer Professional Management System 21 (OPMS XXI). US Army Perscom Online provides Answers to Frequently asked questions about this new personnel system, updated 8 Feb 1999, www.army.mil/smartbook/SmBkFAQ.htm 22 Mar 1999

²⁰ Army.mil/opms/smartbook, Tab C "Frequently Asked Questions, Update 8 Feb 99)

²¹ Jim Tice, " A New Officer Specialty for the Information Age", Army Times 25 Jan 1999: 15

²² Jim Tice, " A New Officer Specialty for the Information Age", Army Times 25 Jan 1999: 15

²³ LTC Ron Garner telephonic interview, 23 April 1999.

²⁴ Carl von Clausewitz, On War, ed. Anatol Rapoport, (London: Penguin, 1988) 162-163.

²⁵ FM100-6, iv

BIBLIOGRAPHY

Clausewitz, Carl Von. On War. ed. Anatol Rapoport, London: Penguin, 1988.

Dunlap, Charles J. Jr. Technology and the 21st Century Battlefield: Recomplicating Moral Life for the Statesman and the Soldier. Carlisle, Strategic Studies Institute: 15 January 1999.

Fredericks, Brian. Information Warfare: The Organizational Dimension. Strategy Research Project. Carlisle: US Army War College, 7 February 1996.

Fredericks, Brian. Personal Interview. 17 December 1998.

Hartzog, William W. Force XXI: Land Combat in the 21st Century. U.S Army Training and Doctrine Command, Virginia: October 1998.

Garner, Ron. Personal Interview. 23 April 1999.

Giffin, John. Personal Interview. 8 February 1999.

Pfaltzgraff, Robert L. Jr. and Richard H. Shultz Jr. War in the Information Age: New Challenges for U.S. Security. Virginia: Brassey, 1997.

Pfaltzgraff, Robert L.Jr. War in the Information Age. Proceedings of Conference hosted by The Institute for Foreign Policy Analysis, Inc. 15 November 1995, Cambridge, The Fletcher School Of Law and Diplomacy. April 1996.

Tice, Jim " A New Officer Specialty for the Information Age", Army Times 25 January 1999: 15

United States. Joint Doctrine for Information Operations. Joint Publication 3-13. Joint Chiefs of Staff, Washington: GPO, 9 October 1998.

—. Information Operations. Field Manual 100-6. Headquarters, Department of the Army, Washington: GPO, August 1996.

—. Joint Vision 2010. Joint Chiefs of Staff, Washington: GPO, 1997.

—. Information Warfare. A Strategy for Peace...The Decisive Edge in War. Joint Chiefs of Staff, Washington: GPO, January 1997.

—. Concept for Future Joint Operations. Expanding Joint Vision 2010. Joint Chiefs of Staff, Washington: GPO, May 1997.

—. Public Affairs Operations. Field Manual 46-1. Headquarters Department of the Army, Washington: GPO, May 1997.

—. America's Army: Preparing for Tomorrow's Security Challenges. Army Issue Paper No. 2, Carlisle, Strategic Studies Institute: November 1998.

—. (OPMS XXI). US Army Perscom Online provides Answers to Frequently asked questions about this new personnel system Tab C, updated 8 Feb 1999, www.army.mil/smartbook/SmBkFAQ.htm. 22 Mar 1999

Winters, Jim. Personal Interview. 8 February 1999.